College Decision 037/2025

DECISION OF THE COLLEGE OF THE EUROPEAN PUBLIC PROSECUTOR'S OFFICE OF 7 MAY 2025

Adopting the EPPO COUNTER-INTELLIGENCE Policy

The College of the European Public Prosecutor's Office (EPPO),

Having regard to the Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'), and in particular Articles 9(2) thereof,

Whereas:

(1) The EPPO recognises the increasingly complex and diverse threats posed by hostile intelligence entities, who are employing a sophisticated blend of traditional espionage, cyber operations, and influence campaigns to steal sensitive information, compromise critical infrastructure, and undermine EU entities.

Has adopted this decision:

Sole Article

(1) The EPPO Counter-intelligence Policy is laid down in the Annex to this Decision, which forms an integral part of this Decision.

(2) This Decision shall enter into force on the day following that of its adoption.

Done at Luxembourg on 7 May 2025.

On behalf of the College,

Qualified electronic signature by: LAURA CODRUȚA KÖVESI
Date 2025-05-08 10:06:03 UTC

Laura Codruța KÖVESI

European Chief Prosecutor

ANNEX

Counter-intelligence Policy

Introduction

Purpose

This Policy aims to establish a robust framework to protect the EPPO from espionage, unauthorised disclosures of information and other intelligence threats that could determine a risk for the organisation.

Related Documents

- Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the EPPO[1] *(Link)*
- Decision 011/2021 of the College of the EPPO of 24 February 2021 on The Protection of EU Classified Information (*Link*)
- Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union (hereinafter referred to as the "Cybersecurity Regulation")
- Decision 013/2024 of the College of the EPPO of 7 February 2024 on the EPPO Single Programming Document for the period 2025-2027 (hereinafter referred to as "College Decision 013/2024") (*Link*)
- Decision 014/2024 of the College of the EPPO of 7 February 2024 on Security Rules applicable to the Digital Communication and Information Systems of the EPPO (hereinafter referred to as "College Decision 014/2024") *(Link)*
- Decision 042/2024 of the College of the EPPO of 26 June 2024 on the Security Strategy 2024-2028 (hereinafter referred to as "College Decision 042/2024") (*Link*)
- Glossary of Administrative Terms and Abbreviations 2.0[2] *(Link)*

[1] OJ L 283, 31.10.2017, p. 1–71.

[2] Decision EPPO/2023/AD/160 of the Administrative Director of the EPPO of 4 June 2023 updating EPPO's Glossary of Administrative Terms and Abbreviations (ref. Ares(2023) 4131648 – 14/06/2023).

Policy

Definitions

For the purposes of this Policy, the definitions of the **Glossary of Administrative Terms and Abbreviations** apply:

EPPO post-holder;

Person;

Service provider.

Some terms used in this policy lack established definitions at the EU level. For clarity, the following NATO definitions are considered as reference:

Counter-intelligence[3] (CI) is defined as those activities that identify the threat to security posed by hostile intelligence services or organisations or by individuals engaged in terrorism, espionage, sabotage, subversion, organised crime or other non-traditional threats.

CI personnel – within Security Unit, individuals with expertise on CI matters, responsible for detecting, preventing, and neutralizing threats posed by hostile intelligence services, insider threats, and other adversarial activities that could compromise EPPO's sensitive information.

Espionage[4] – intelligence activity directed towards the acquisition of information through clandestine means and proscribed by the law.

Hybrid threat[5] – a type of threat that combines conventional, irregular and asymmetric activities in time and space.

[3] As defined in Allied Administrative Publication AAP-06, "NATO Glossary of Terms and Definitions", edition 2021.
[4] Ibid.
[5] Ibid.

Hostile Intelligence Service[6] (HoIS) – known or suspected intelligence entity that conducts activities aimed at gathering information about an organisation, disrupting its operations, or influencing its decision-makers.

Information[7] – in intelligence, unprocessed data of every description, which may be used in the production of intelligence.

Intelligence[8] is the product resulting from the processing of information.

Open Source Intelligence[9] (OSINT) - intelligence based on information collected from sources open to the public, such as radio, television, newspapers, state propaganda, learned journals, technical manuals and manuals, books, and online information.

Organised Crime[10] (OC) may be described as the actions of organisations of a criminal nature, structured as a network, with one or more leaders and several subordinate units spread over a large territory.

Sabotage[11] – the intentional destruction, disruption or disabling of equipment/systems, materials and facilities by or for a hostile element.

Subversion[12] – action designed to weaken the strength of an organisation by undermining the morale, loyalty or reliability of its employees.

Technical Surveillance Countermeasures (TSCM)[13] – techniques used to prevent, detect and neutralise hostile intelligence efforts to obtain information through the introduction of a monitoring device or the exploitation of weaknesses in Technical Secure Areas.

Scope

This policy applies to all EPPO Staff. For the purpose of this policy, '*Staff*' means EPPO post-holders and long-term service providers, including trainees and interims.[14]

[6] As described in Allied Joint Publication (AJP) 2.2 - "Allied Joint Doctrine for Counter-intelligence".
[7] As defined in EEAS(2023)914 REV4, EUMC Glossary of Acronyms and Definitions, revision 2023.
[8] Ibid.
[9] Ibid.
[10] As defined in Allied Command Operations (ACO) Directive 065-003 "Counter-intelligence Policy in NATO ACO".
[11] Ibid.
[12] Ibid.
[13] Ibid.
[14] See the Glossary of Administrative Terms and Abbreviations 2.0 for the definitions of EPPO post-holders and long-term service providers.

This policy covers the main CI functions (i.e. CI Awareness and Training, Network and Cooperation, Risk Assessment and Security Inquiry), envisioned for an effective CI program focused on protecting the EPPO.

Organisation and Mission

The EPPO CI capability functions within the Security Unit.

CI seeks to identify, exploit and counter the threats posed by Terrorism, Espionage, Sabotage, Subversion and Organised Crime (TESSOC), against the EPPO personnel, information, and assets, therefore **contributing to security**.

CI Services

CI uses a multi-discipline approach to identify threats posed to the EPPO. CI personnel will perform routine functions / capabilities which include, but are not limited to, the following:

CI Awareness and Training

In consultation with the HR Unit, CI personnel shall deliver mandatory induction and periodic tailored training sessions to equip staff with the necessary skills to identify potential threats and adhere to reporting procedures for suspicious activities.

CI personnel shall deliver ad-hoc[15] pre-travel briefings to staff undertaking duty travels to sensitive destinations, aiming to raise awareness of potential risks and provide them with strategies to mitigate these risks, ensuring the security of both personal and institutional information during their trip.

Network and Cooperation with Third Parties

CI personnel shall establish and continue strengthen liaison relationships with counterparts from:

a) EU Institutions, Office, Bodies, and Agencies (EU IBOAs).
b) National Security Authorities (NSAs) - security, intelligence, counter-intelligence, counter-terrorism, investigative services - from Member States.

[15] Event-driven.

c) International organisations (NATO, UN offices, etc.).

CI personnel shall be actively involved in security / intelligence / CI working groups convened at EU level to be acquainted with all CI dynamics and exchange best practices in the field.

CI personnel shall establish adequate collaboration channels with other EPPO units to ensure work efficiency and enhance information sharing.

In the spirit of collaboration, the European Prosecutors (EP) and European Delegated Prosecutors (EDP) should contribute, on a best effort basis, to the EPPO CI objectives[16] by facilitating the liaison between EPPO CI personnel and national security authorities that could be contacted for additional support elements.

CI Risk Assessment

CI personnel shall contribute to the necessary analytical processes to assess the risk level of threats that may have an impact on EPPO.

Self-threat assessment questionnaire

To ensure a comprehensive and accurate assessment of the threat landscape, CI personnel shall develop effective mechanisms to identify CI and hybrid threats with impact on the EPPO Staff and operations. The fundamental tool is the self-threat assessment questionnaire which must be distributed to EPPO personnel involved in operational tasks, with the aim to gather specific insights and feedbacks.

Personal Threat Assessment Review

As part of the CI risk framework, CI personnel shall conduct regular interviews with European Chief Prosecutor, European Prosecutors, and any other person involved in operational tasks for monitoring their personal threat levels indicated in Personal Threat Assessments. Following a risk-based approach, the minimum frequency of the interviews depends on the initial / previous threat level:

a) LOW level - annual interview.

b) MODERATE level - bi-annual interview.

[16] As defined in the "College Decision 013/2024" and the "College Decision 042/2024".

c) SUBSTANTIAL level – quarterly interview.

d) Whenever the situation requires: ad-hoc interviews.

Security Inquiries

CI personnel shall conduct inquiries only when mandated by the Security Authority and under the supervision of the Head of the Security Unit. These inquiries may be initiated in response to incidents affecting EPPO's security or upon detection of counterintelligence indicators, including but not limited to espionage, foreign interference, and unauthorized information disclosure.

In such cases, CI personnel shall be permitted to carry out all necessary investigative activities, as authorized by the Security Authority, to clarify the circumstances surrounding an incident and present factual findings.

CI personnel may also make use of Open-Source Intelligence (OSINT) methods, tools and sources, as authorized by the Security Authority, to support security inquiries or other fact-finding activities.

Upon completion of a security inquiry, CI personnel shall prepare a report outlining the key fact-findings and conclusions. This report shall be submitted for approval to the Head of the Security Unit, who will oversee its dissemination as required.

Following the adoption of this policy, CI personnel shall develop practical guidelines outlining the procedures for conducting security inquiries at EPPO level.

Personal data processed in the context of security Inquiries shall comply with the provisions outlined in the Record of Processing Activity (RoPA) for Administrative inquiries and disciplinary proceedings[17].

Technical Surveillance Countermeasures (TSCM)

CI personnel shall coordinate all TSCM activities that are envisaged to be performed at EPPO level and shall take appropriate measures to ensure the execution of this specialised service.

Responsibility

Ownership

[17] Processing record no. APD-201021-AD.

The Security Authority is the owner of this Policy.

Actors and Roles

The Security Authority shall be responsible in defining the distribution and accessibility of the reports / analytical products issued by the CI personnel.

The Head of the Security Unit shall be responsible in ensuring that CI personnel perform the following activities:

a) Raising awareness on all issues related to CI / hybrid threats at EPPO level.

b) Collecting relevant information to assess specific threats and risks which may impact EPPO staff, operations and assets.

c) Ensuring external liaison with other EU IBOAs, NCAs and international organisations.

d) Conducting security inquiries of CI related incidents.

The HR Unit shall be responsible for planning the CI training sessions, while each **Head of Unit and Head of Sector** shall ensure that all post-holders, long-term service providers and trainees have attended the required CI awareness sessions, briefings and trainings.

The Staff shall attend the required CI awareness sessions, briefings and trainings and follow the instructions related to the implementation of this Policy.